

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows:

- C¹
1. (Currently Amended) A method for encrypting data, the method comprising:
providing a data processing system for:
generating a session key;
encrypting the data utilizing the session key;
encrypting the session key utilizing a user public key;
encrypting the session key utilizing a master public key;
generating a data packet including the encrypted data, ~~and the encrypted~~
session key utilizing the user public key and the encrypted session
key utilizing the master public key;
transmitting the data packet to a destination data processing system;
decrypting the data packet utilizing the session key;
decrypting the session key utilizing a user private key; and
decrypting the encrypted session key utilizing a master private key.
~~an authorized party accessing the encrypted data by utilizing the master~~
~~public key and a master private key; and~~
~~the authorized party decrypting the encrypted session key utilizing the~~
~~master private key and decrypting the encrypted data with the~~
~~session key to recreate original data.~~
 2. (Cancel).
 3. (Cancel).

4. (Original) The method, as set forth in claim 1, further comprising encrypting the session key utilizing an asymmetric encryption routine.
5. (Original) The method, as set forth in claim 1, further comprising encrypting the data utilizing a symmetric encryption routine.
6. (Cancel).
7. (Currently Amended) The method, as set forth in claim-21, further comprising storing a user's private key on a data storage medium coupled to the destination data processing system.
8. (Previously Amended) The method, as set forth in claim 1, further comprising storing the master private key on a data storage medium coupled to the destination data processing system.
9. (Previously Amended) The method, as set forth in claim 7, further comprising retrieving the user's private key from a smart card utilizing a smart card reader coupled to the destination data processing system.
10. (Previously Amended) The method, as set forth in claim 1, further comprising retrieving the master private key from a smart card utilizing a smart card reader coupled to the destination data processing system.
11. (Original) The method, as set forth in claim 1, further comprising utilizing a plurality of public master keys and a plurality of private master keys to decrypt the encrypted session key.

12. (Currently Amended) A public key data encryption system wherein each user has a private key and a certificate containing data pertaining to the user including the user's public key, the encryption system comprising:
a master public key;
a first data processing system operable to generate a session key, to encrypt data using the session key, to encrypt the session key with the user's public key, to encrypt the session key with the master public key, to generate a data packet including the encrypted session keys and the encrypted data, and to transmit the data packet to a second data processing system;
the second data processing system operable to:
decrypt the data packet utilizing the session key;
decrypt the session key utilizing a user private key; and
decrypt the encrypted session key utilizing a master private key.
~~an authorized party accessing the encrypted data by utilizing the master public key and a master private key; and~~
~~the authorized party decrypting the encrypted session key utilizing the master private key and decrypting the encrypted data with the session key to recreate original data.~~
13. (Cancel).
14. (Cancel).
15. (Original) The public key data encryption system, as set forth in claim 12, wherein an asymmetric encryption routine is utilized to encrypt the session key.

- C1
16. (Original) The public key data encryption system, as set forth in claim 12, wherein a symmetric encryption routine is utilized to encrypt the data.
 17. (Cancel).
 18. (Previously Amended) The public key data encryption system, as set forth in claim 12, wherein the user's private key is stored on a data storage medium coupled to the second data processing system.
 19. (Previously Amended) The public key data encryption system, as set forth in claim 12, wherein the master private key is stored on a data storage medium coupled to the second data processing system.
 20. (Previously Amended) The public key data encryption system, as set forth in claim 12, further comprising a smart card reader coupled to the second data processing system and operable to retrieve the user's private key from a smart card.
 21. (Previously Amended) The public key data encryption system, as set forth in claim 12, further comprising a smart card reader coupled to the second data processing system and operable to retrieve the master private key from a smart card.
 22. (Currently Amended) The public key data encryption system, as set forth in claim 12, further comprising:
a plurality of master private keys; and
a plurality of master public keys; ~~and~~

~~a second data processing system operable to receive the data packet, to decrypt the encrypted session key with the plurality of master private keys, and to decrypt the data with the session key.~~

23. (Currently Amended) An article of manufacture comprising:
a computer usable medium having computer readable program code embodied therein for encrypting and decrypting data wherein each user has a private key and a public key, the article of manufacture comprising:
a master public key;
a first data processing module operable to generate a session key, to encrypt data using the session key, to encrypt the session key with the user's public key, to encrypt the session key with the master public key, to generate a data packet including the encrypted session keys and the encrypted data, and to transmit the data packet to a second data processing module;
the second data processing module operable to:
decrypt the data packet utilizing the session key;
decrypt the session key utilizing a user private key; and
decrypt the encrypted session key utilizing a master private key.
~~an authorized party accessing the encrypted data by utilizing the master public key and a master private key; and~~
~~the authorized party decrypting the encrypted session key utilizing the master private key and decrypting the encrypted data with the session key to recreate original data.~~

24. (Cancel).

25. (Cancel).

- C1
26. (Previously Amended) The article of manufacture, as set forth in claim 23, wherein an asymmetric encryption routine is utilized to encrypt the session key.
27. (Previously Amended) The article of manufacture, as set forth in claim 23, wherein a symmetric encryption routine is utilized to encrypt the data.
28. (Cancelled).
29. (Currently Amended) The article of manufacture, as set forth in claim 23, further comprising:
a plurality of master private keys; and
a plurality of master public keys; and
~~a second data processing module operable to receive the data packet, to decrypt the encrypted session key with the plurality of master private keys, and to decrypt the data with the session key.~~
-